



Mail: P. O. Box 5231, Princeton, NJ 08543-5231

Princeton Pike Corporate Center, 997 Lenox Drive, Lawrenceville, NJ 08648-2311
Tel (609) 896-3600 Fax (609) 896-1469

101 Park Avenue, 17th Floor, New York, NY 10178
Tel (212) 878-7900 Fax (212) 692-0940
www.foxrothschild.com

DOMINIQUE J. CARROLL
Direct No: (609) 895-6706
Email: DJCarroll@FoxRothschild.com

August 10, 2023

Via ECF

Hon. Christine P. O’Hearn, U.S.D.J.
United State District Court
District of New Jersey
Mitchell H. Cohen Building
& U.S. Courthouse
4th & Cooper Streets
Camden, NJ 08101

Re: *The HomeSource Corp. v. Retailer Web Services, LLC et al.*

Dear Judge O’Hearn:

We represent Defendants Retailer Web Services, LLC and Retailer Web Services II, LLC (together, “RWS”), and provide the Court with a case status pursuant to ECF No. 343.

I. Relevant Background

RWS sent a newsletter in July 2018 about the owners of Plaintiff The HomeSource Corp. and their predecessor companies having a litigious background. The very next business day, HomeSource sued RWS and claimed it was damaged over \$46 million by the newsletter.

HomeSource claimed that the newsletter defamed it, and that it tortiously interfered with unspecified contracts and business opportunities. ECF No. 1. A few weeks later, HomeSource filed its First Amended Complaint (“FAC”) and accused RWS of committing cyberattacks against its customers’ websites. ECF No. 12. 5 years later, HomeSource still has not provided RWS with any evidence to support these incendiary allegations, despite RWS’s exhaustive efforts to get it.

HomeSource then sought to amend its complaint three more times, before filing the operative Second Amended Complaint (“SAC”). ECF No. 164. In the SAC, HomeSource again alleges that RWS perpetrated cyberattacks, and added a claim under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.* (“CFAA”) (Count VI). HomeSource’s claims all stem from two general acts: (1) that the July 2018 newsletter hurt HomeSource, and (2) cyber-allegations.

A Pennsylvania Limited Liability Partnership

California Colorado Delaware District of Columbia Florida Georgia Illinois Massachusetts Minnesota Missouri Nevada [New Jersey](#) New York North Carolina Oklahoma Pennsylvania South Carolina Texas Washington



Hon. Christine P. O'Hearn, U.S.D.J.
Page 2 of 4

A. The Court Rebuffs HomeSource’s Motion For Partial Summary Judgment On The Defamation And Lanham Act Claims.

On February 22, 2022, the Court denied HomeSource Motion for Partial Summary Judgment on its defamation and Lanham Act claims (ECF No. 290) in its entirety. It found that (1) HomeSource lacked standing to pursue its claims for 2 of the 4 statements, (2) the third statement was not literally false or libelous *per se*; and (3) HomeSource failed to produce any evidence of injury caused by the fourth statement. ECF No. 309. Despite being rejected, HomeSource is *still* maintaining the denied claims against RWS. And over a year and half later, HomeSource has provided no evidence that the fourth statement *caused* it any damage, or that it was anything more than a minor inaccuracy.

B. HomeSource Pursues Cyber-Allegations For 5 Years Without Any Evidentiary Or Factual Support For Them.

Within days of HomeSource raising its cyber-allegations, RWS’s counsel offered to help investigate the cyber-allegations and asked for evidence supporting them. *See* Ex. 1 (RWS’s Sept. 8, 2018 Letter to HomeSource). Despite the seriousness of the cyber-allegations raised against RWS, HomeSource refused to provide access to its alleged evidence. After over 50+ attempts, RWS was forced to seek court intervention. After then-Magistrate Judge Williams held a discovery conference on October 7, 2019 (ECF No. 127), she found HomeSource’s discovery responses deficient and compelled HomeSource to, among other things:

- “[M]ake the ‘mirror image’ of the database available to defendant’s expert.”
- “[P]rovide an affidavit or certification detailing all information” HomeSource possess regarding the alleged hacking and/or cyber-attacks and/or denial of service and/or distributed denial of service attacks.

Oct. 16, 2019 Order (ECF No. 129) at 4 ¶¶ 5-6.

HomeSource still refused to provide access to the “mirror image” of its database. Because of HomeSource’s stonewalling, RWS filed a second motion to compel in December 2020. *See* ECF No. 254. Judge Robreno, on March 5, 2021, also ordered HomeSource to provide RWS’s expert with access to the mirror image of HomeSource’s database. ECF No. 264. Yet HomeSource continued to refuse to produce evidence supporting its cyber-allegations and CFAA claim, including access to the mirror image of its database.

After nearly five years of RWS fighting to get access to the Court Ordered discovery, Special Master Orlofsky ruled that “HomeSource has failed to comply with Judge Williams’ and Judge Robreno’s Orders regarding the creation, maintenance, and production of a ‘mirror image’ of its database.” ECF No. 325 at 1. Whatever HomeSource had claimed it saved, it was not a mirror image of the computer system allegedly attacked, and “does not comply with Judge Williams’ Order, and in fact was not even created *in response* to that order.” ECF No. 325 at 10



Hon. Christine P. O’Hearn, U.S.D.J.
Page 3 of 4

(emphasis in original).

Indeed, what HomeSource calls its “snapshot” that it saved wasn’t even *created* until December 2018, which is months after the alleged August 2018 cyberattacks, and “approximately 9 months before the September 29, 2019 cyberattacks.” *Id.* The Special Master also found that HomeSource’s claims “beg the question of what evidence could possibly be contained in the snapshot that supports those claims” if they were created that long after, or even *before* some of the alleged cyberattacks. *Id.* The Court also stated that the “snapshot” that HomeSource created “cannot be searched in the manner that Judge Williams directed, nor can it authenticate the underlying source of the data [*i.e.*, the allegedly attacked web server].” *Id.* at 11.

HomeSource has since confirmed that the Web Server (the system alleged attacked) as it existed at the times of the claimed cyberattacks has been destroyed and no longer exists. *Id.* at 8.

II. Status of Discovery And Pending Motions

Discovery here was exasperated by HomeSource’s refusal to produce evidence of its cyber-allegations and CFAA claim. Because of HomeSource’s years of discovery misconduct, RWS filed a motion for discovery sanctions (ECF No. 327) and a motion for sanctions under Rule 11 (ECF No. 330). The motion for discovery sanctions is fully briefed, and the Rule 11 motion will be fully briefed on **August 11, 2023**. Special Master Orlofsky informed the parties that he will consider the pending sanctions motions.

The pending motion to seal (ECF No. 307) also remains undecided, and RWS proposes that it be submitted to Special Master Orlofsky for resolution.

The parties have completed all fact witness depositions, except for one Rule 30(b)(6) Deposition of RWS, and limited written and document discovery of non-party Phyllis White. *See* ECF No. 344 (granting in part, and denying in part, Ms. White’s Motion to Quash).

On August 10, 2023, Special Master Orlofsky entered a Ninth Scheduling Order setting the following remaining case deadlines (ECF No. 345):

Description of Deadline	Proposed Deadline
Completion of fact discovery	August 25, 2023
Affirmative expert report(s) due	October 6, 2023
Rebuttal expert report(s) due	November 3, 2023
Completion of expert discovery	December 1, 2023



Hon. Christine P. O'Hearn, U.S.D.J.
Page 4 of 4

Affirmative motions for summary judgment	January 12, 2023
Responses to motions for summary judgment	February 9, 2024
Replies in support of motions for summary judgment	March 1, 2024

RWS appreciates this opportunity to provide a case update to the Court.

Respectfully submitted,

A handwritten signature in blue ink that reads "Dominique J. Carroll".

Dominique J. Carroll

Enclosures

cc: All counsel of record (via ECF)